



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/260,796	03/01/1999	JAMES P HUGHES	98-019-NSC	6934

7590 02/22/2005

TIMOTHY R SCHULTE  
STORAGE TECHNOLOGY CORPORATION  
2270 SOUTH 88TH STREET MS-4309  
LOUISVILLE, CO 800284309

EXAMINER

DARROW, JUSTIN T

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 02/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/260,796

Applicant(s)

HUGHES, JAMES P

Examiner

Justin T. Darrow

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 29 October 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☒ Claim(s) 13-17 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 01 March 1999 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)             | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                                    |

**DETAILED ACTION**

1. Claims 1-17 have been examined.

***Drawings***

2. The drawings filed on 03/01/1999 are acceptable to the examiner and the draftperson.

***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4. Claims 1 and 2 are rejected under 35 U.S.C. 102(a) as being anticipated by Canal Societe Anonyme (Maillard et al.), International Application Publication No. WO 98/43425 A1.

Art Unit: 2132

As per claim 1, Maillard et al. illustrate a method for secure handling of information comprising:

decrypting a value required to decrypt information (see page 21 and figure 9, item 3156),  
the value decrypted by correctly solving an access formula describing a function of groups, each group comprising a list of at least one client, wherein the requesting consumer client is granted access to the information if the requesting consumer client is a member of at least one group which correctly solves the access formula (see page 21 and figure 9, items 3152 and 3154).

As per claim 2, Maillard et al further describes:

that the encrypted value and the access formula are stored as metadata in the data set (see page 20 and figure 7, step 3142).

5. Claims 3, 4, and 6-12 are rejected under 35 U.S.C. 102(e) as being anticipated by Langford et al., U.S. Patent No. 6,266,420 B1.

As per claim 3, Langford et al. describe a method for secure handling of information, comprising:

creating at least one group, each group comprising a list of at least one consumer client (see column 3, lines 14-22; figure 2, item 14);

acquiring a public key and a matched private key for each of the at least one group (see column 3, lines 53-55; figure 3, step 40);

Art Unit: 2132

encrypting an information set to produce a data set, based on a randomly generated number (see column 3, lines 18-20; figure 2, item 20);

determining access expressed as a logical combination of at least one group for which access to the information will be granted, solved by the indication that the consumer client belongs to that the at least one group (see column 3, lines 35-38; figure 2, item 30);

asymmetrically encrypting the randomly generated number using access determination and the public key for each of the at least one group granted access to the information set (see column 3, lines 20-22; figure 2, item 14);

adding the encrypted randomly generated number to the data set (see column 3, lines 22-25; figure 2, items 18, 20, and 22); and

storing the data set on at least one untrusted storage device (see column 3, lines 25-27).

As per claim 4, Landford et al. further point out:

receiving a request from the consumer client (see column 3, lines 31-33; figure 2, item 24);

determining if the consumer client belongs to at least one group and, if not, denying access (see column 3, lines 36-38);

decrypting the randomly generated number using the private key for the at least one determined group (see column 4, lines 14-17; figure 3, step 46; column 3, lines 38-40; figure 2, items 22 and 30); and

Art Unit: 2132

encrypting the randomly generated number using the public key for the consumer client permitting access to the encrypted information set by the consumer client (see column 4, lines 38-40; figure 3, step 50; figure 2, item 28).

As per claim 6, Langford et al. additionally embody:

multiple group private decryption keys for different groups (see column 3, lines 40-43);

decrypting the randomly generated number using the private key for the at least one determined group (see column 4, lines 14-17; figure 3, step 46; column 3, lines 38-40; figure 2, items 22 and 30); and

encrypting the randomly generated number using the public key for the consumer client permitting access to the encrypted information set by the consumer client (see column 4, lines 38-40; figure 3, step 50; figure 2, item 28).

decrypting the reencrypted partial key using the private key of the requesting client (see column 4, lines 52-56); and

decrypting the information set using the determined randomly generated number (see column 4, lines 52-56).

As per claim 7, Langford et al. then point out:

that the determination that the client belongs to the group is true (see column 3, lines 36-38).

As per claim 8, Langford et al. additionally describe:

Art Unit: 2132

determining that an information set destined for storage on at least one untrusted storage device is encrypted (see column 4, lines 40-42; figure 3, step 52); and

prohibiting storage on the at least one untrusted storage device if the information set is determined not to be encrypted (see column 4, lines 48-56).

As per claim 9, Langford et al. depict a system for the secure handling of information, comprising:

a key manager operable to generate private and public key pairs (see column 3, lines 20-22; figure 2, item 22; column 3, lines 36-38);

at least one group server operable to

(a) maintain at least one group comprising a list of client members allowed to access information (see column 3, lines 20-22; figure 2, item 14);

(b) obtain a private key and matched public key for each group (see column 3, lines 20-22; figure 2, item 22; column 3, lines 36-38); and

at least one producer client operative to

(a) encrypt an information set to produce a data set based on an encryption value (see column 3, lines 18-20; figure 2, item 20);

(b) determine access expressed as a logical combination of at least one group for which access to the information will be granted, solved by the indication that the client belongs to that the at least one group (see column 3, lines 35-38; figure 2, item 30);

Art Unit: 2132

(c) asymmetrically encrypt the encryption value using access determination and the public key for each of the at least one group granted access to the information set (see column 3, lines 20-22; figure 2, item 14);

(d) add the encrypted encryption value to the data set (see column 3, lines 22-25; figure 2, items 18, 20, and 22); and

(e) store the data set on at least one untrusted storage device (see column 3, lines 25-27).

As per claim 10, Langford et al. suggest:

that the encryption value comprises a randomly generated number (see column 1, lines 10-26).

As per claim 11, Langford et al. then point out:

that the determination that the client belongs to the group is true (see column 3, lines 36-38).

As per claim 12, Langford et al. additionally describe:

determining that an information set destined for storage on at least one untrusted storage device is encrypted (see column 4, lines 40-42; figure 3, step 52); and

prohibiting storage on the at least one untrusted storage device if the information set is determined not to be encrypted (see column 4, lines 48-56).



Art Unit: 2132

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Langford et al., U.S. Patent No. 6,266,420 B1 as applied to claim 4 above, and further in view of Carter, U.S. Patent No. 5,787,175 A.

As per claim 5, Langford et al. disclose the method of claim 4. Carter suggests that the attempt to access the document is logged (see column 16, lines 44-50). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method of Langford et al. with the audit trail of Carter to foil unauthorized decryption attempts (see column 5, lines 62-67).

***Allowable Subject Matter***

8. Claims 13-17 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

9. The following is a statement of reasons for the indication of allowable subject matter:

Art Unit: 2132

Claims 13-17 are drawn to a system for the secure handling of information. The closest prior art, Langford et al., U.S. Patent No. 6,266,420 B1, disclose a similar system. However, they neither teach nor suggest sending a request to access the encrypted information set to each of the at least one determined group server and decrypting the encryption value using the obtained private key if access is granted from each of the determined at least one group server. This composite sequence of steps explicitly recited in intervening claim 13 renders claims 13-17 to have allowable subject matter

### *Telephone Inquiry Contacts*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (703) 305-3872 and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

The fax numbers for Formal or Official faxes to Technology Center 2100 are (703) 305-0040 and (703) 746-7239. Draft or Informal faxes for this Art Unit can also be submitted to (703) 746-7240. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and

Art Unit: 2132

consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 746-7238 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only **"OFFICIAL FAX"** but also **"AMENDMENT AFTER FINAL"**.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900.

February 18, 2005

*Justin Darrow*  
**JUSTIN T. DARROW**  
**PRIMARY EXAMINER**  
**TECHNOLOGY CENTER 2100**